1. Introduction To Computer And Information Security

-1-24

* Need of computer Security -

(Basic concept of NIS)
1) confedentiality
2) Integrity
3) Availability

1) Protect sensitive information.
2) Preventing dataloss.
3) Maintaining system availability
4) Compliance with regulations
5) Protect against cyberattack.
6) Preserving privacy

(explain three pillars of security ?)

* Basic Concept Of NIS -

1) Confedentiality - it Refers to the protection of sensitive information from unauthorized access or disclosure
- Tools to acheive confidentiality is cryptography.

2) Integrity - In computer security integrity refers to preservation of accuracy and consistency of data over its entire lifecycle. It assures that data cannot be altered or destroyed by unauthorized individuals and that remains intacts from its original form

3) Availability - In computer security refers to the ability of authorized individual to access the data as and when required. This includes insuring that systems are functioning properly and are not subject to disruption. such as - downtime, dataloss or unavaliability.

10-01-24

4) Accountability - In computer security accountability refers to ability of assigning responsibility for actions taken in a computer system.
- It involves insuring that individual are held accountable for their action and that the system can accurately track and record their activities.

~~Scissor~~

* Ceaser cipher -

- In ceaser cipher we increase a plain text by given a key value.
- The formula used in ceaser cipher is

$$CT = (PT + Key) \bmod 26$$

- In traditional ceaser cipher key value is 3.
- To decript the CT we used - $PT = (CT - Key) \bmod 26$

5) Non-repudiation - Non-repudiation it refers to the ability to prevent individual from denying their actions or authenticity of electroni transaction.

- It is a key component of secured communication and it is used t ensure that sender of a message cannot later deny having send it and the receipient of message cannot deny having receive it.
- Techniques -
  1. Digital signature
  2. Public key Infrastructure.
  3. Secured hash function.

6) Reliability - It refers to the ability of a system to perform its inteded function in an consistent and dependable manner.

- It is major of stability and dependability of a system and is an important consistration and insuring of the availability and functionality of system and data.

7) Authentication - It is a process of verifying identity of user, device, system.

- The goal of Authentication is to ensure that only authorised user have access to the resources or information.

8) *. Access Control -

- It is a process of regulating who and what can view or update in the system.
- It determines who is allow to access specific resources and what they are allow to do with these resources.
- There are several types of access control method:-

1) Rolebase access control (RBAC):

A method of access control that give ~~the owner of the resource the abiltity to determine who is allowed to access~~. grant access to resources based on role or job function of the user.

2) Discriptionary Access Control (DAC) -

A method of access control that give the owner of the resource the ability to determine who is allowed to access.

3) Mandatory Access Control (MAC) -

A method of access control that inforces the pre-determine set of rules to determine who is allowed to access resources.

4) Rule based Access control (RBAC) -

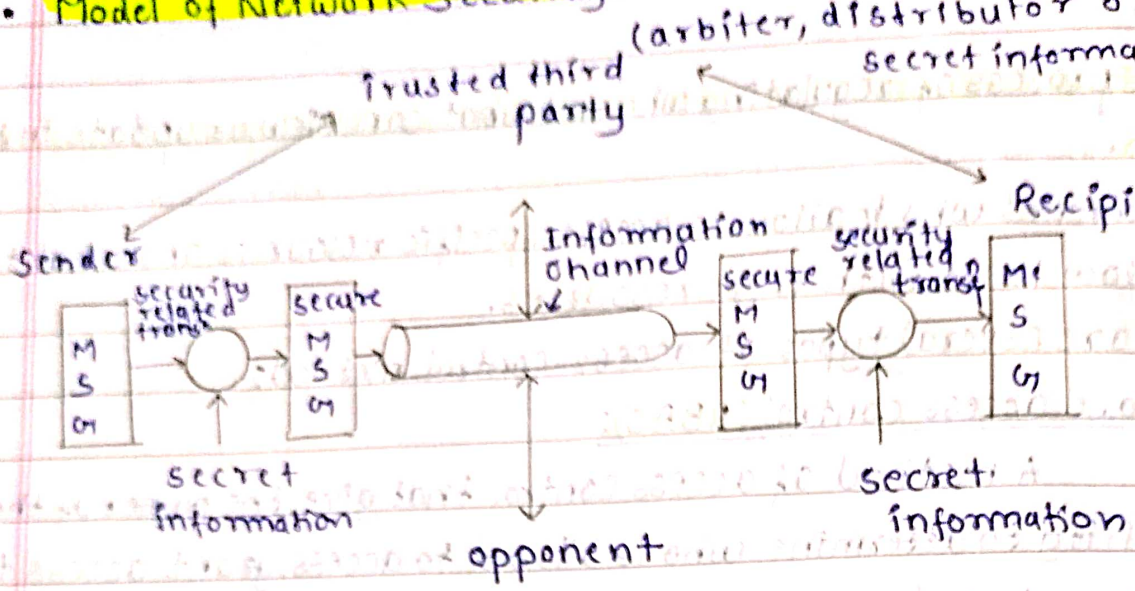
A method of access control that uses a set of rule to determine who is allow to access resources.

5) Attribute based Access control (ABAC) -

Method of access control that grant access to the resource based on the attribute of the user such as their location, time of access and other factor.

⇒ Access control is important because it help to ensure that sensitive information and resource are protected and can only accessed by the authorised Individual. This helps to prevent unauthorised access, data breaches and other security incidence.

- Model of Network Security -



* Risk - Risk refers to ~~pote~~ potential harm or lost of data or infor that arises from use of technology and inform system.
- Risk can come from various resources including hardware and software failure, natural disasters, millicious attacks and human er

* Threats - These are potential security incidences that put exploid vulnerabilities in a system and caused harm or loss.
- Threats can come in many forms - viruses, malware, denial of service attacks, ~~pishing~~ phishing
- By identifying and mitigating risk and threats organization can protect their system and data from security incidences, minimize the potential impact of security incidences and ensure the confidentiality, integrity, availability of their system and data.

** Risk assesement -
Their are 2 types -
i) Quatitative risk assesement
ii) Qulitative risk assesement.

i) Quantitative risk assesement - It is systematic process use to evaluate and prioritize risk based on their likelyhood of their occurences and potential impact.

. The goal of quantitative risk assesement is to provide detailed and accurate understanding of the risk.

Steps -

① Identify potential risk
② Access likelyhood and impact
③ Calculate risk
④ priotize the risk.

ii) Qualitative risk assesement - It is a process use to evaluate and priotize risk based on expert opinion and subjective judgement.

* Types of Threats -

1) Malware - virus, worms, Torjan horse, Intruders, Insiders.
2) Hacking - Black hat hacker, white hat hacker, Grey hat hacker.
3) Social engineering - Manipulating individuals into sharing sensitive information or performing actions that put the system at risk.
4) Phishing -
5) Insider threat -
6) Physical threat -
7) Denial of Service attack -

* Virus -

Virus is a code or program that attaches itself to another code or program which cause damage to computer system or to computer ~~sys~~ network.

(Phases)

* Stages of Virus -

1) Dormant phase - The virus is idle and can be activated by some event
2) Propogation Phase - It places an identical copy of itself into othe programs or into certain system area on the disk.
3) Trigering phase - The virus is activated to perform the funct for which it was intended.
4) Execution phase - The virus performs the intended function.

Que) * Difference between virus and worms

Virus	Worms
• Virus is the program or code that attaches itself to an application program and when application program runs it runs along with it.	• Worms are code or program that replicates itself in orde to consume resources to bring the system down.
• It inserts itself into a file or executable program.	• It exploids weakness in an application or operating system replicating itself.
• It has to relie on user to transfer infected file or program to other computer system.	• It can use a network to repli itself to other computer system without users intermention.
• Usually delets or modify files or sometime changes file location.	• Usually donot delete or modify file but monopalize CPU and memory. (over utilize)
• Virus is slower than worms.	• Worms is faster than virus.

* Types of virus -

1) parasitic virus -
   • It attaches itself to execute code and replicate itself when infected it will execute and find another program to infect.

2) Memory resident virus -
   • This type of virus lives in the memory after execution. It inserts itself as a part of operating system and manipulate any file that is executable

3) Non-resident virus -
   • This type of virus execute itself and terminate after sometime.

4) Boot sector virus -
   • This type of virus infects the boot record and spread through a system when system is booted from disk.

5) Overwriting virus -
   • This type of virus overwrites the code with its own code.

6) Stealth virus -
   • It is a virus which hides modification it has made in file or boot record.

7) Macro virus -
   • It affects microsoft word document can be spread through mail or other means.

8) Polymorphic virus -
   • It produces fully operational copy of itself in attempt to avoid signature detection.

g) Email virus -

- Virus which gets executed when email attachement is open. virus send itself to everyone in the mailing list of the receiv

* Trojan Horse -

1) It is malicious software program that disguyses itself a legitimate software.
2) It can be used to steal sensitive information, take control of a de or perform other harmful actions.
3) Trojans are often delivered through email attachements, downlo from untrusted websites, or by exploiting vulnerabilities in th software.
4) once installed on a device they can operate silently in the back and can be difficult to detect and remove.

* Intruders - (outsiders)

- Intruder is someone who gaves unauthorized access to a compu system network or device.
- They can use these access to steal benesitive inform cause damag or perform other malicious activities.
- Intruders can exploid vulnerabilities, guess passwords, or use other techniques to bypas security mechanism.
- To protect agains intruders use ~~ster~~ strong password, regularly upd software, and be vigilant for suspicious activity.

* Insiders -

- Insiders refers to a person who has authorised access to an organisations computer system, network or data but uses this access

for malicious purpose.

- Insider are more dangerous because they often have deep understanding of the organizations system and data.
- To mitigate the risk of insider organization should implement strict access control, regularly monitoring system activity and educate employees on security policies, and the importance of protecting sensitive information.

* Vernam Cipher -

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	A	B	C	D	E	F	G	H	I	J	K			
B	B	C	D	E	F	G	H	I	J	K	L			
C	C	D	E	F	G	H	I	J	K	L	M			
D	D	E	F	G	H	I	J	K	L	M	N			

Ex →

PT → ABCD

K → DEC

PT → A B C D A

K → D E C D E

CT → D F E G E

* Railfence (Transposition cipher)

level - 2, 3 (single slope)

→ 1 C M U E S C R T

→ 2 O P T R E U I Y

CT - CMUESCRTOPTREUIY

(DUAL SLOPE)

Level-3

→ 1 C U S R

→ 2 O P T R E U I Y

→ 3 M E C T

CT - CUSROPTREUIYMECT

* Single Columnr Transposition -

PT - Computer security

→ 5 1 3 4 2

5 1 3 4 2

C O M P U

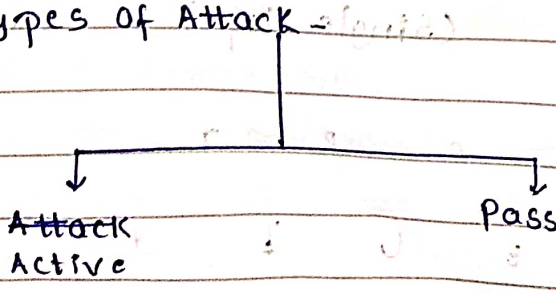
T E R S E

C U R I T

Y X X X X → Fillers

CT - OEUXUETXMRRXPSIXCTCX

* Types of Attack -



• Active attack - It is a type of cyber-attack in which a attacker attempts to alter or destroy data on a targeted

System.

ii) At active attacks are design to disrupt the normal functioning of the system.

iii) Active attacks can cause significant damage to the system.

iv) It results in loss or theft of sensitive information.

Example-

i) Denial of service attack

ii) man in minal attack

iii) reblay attack

- Passive attack- In this attack attacker gathers information from a targeted system or network without altering or disrupting its normal functioning.

ii) Passive attacks are designed to gather sensitive infor^{n} or monitor activity on the system.

iii) Passive attacks are difficult to detect since they donot cause immediate harm to the system.

iv) They result in theft of sensitive infor^{n} and loss of privacy. to protect against this attack we use incription and secure communication protocols.

Example-

i) Eaves dropping

ii) Monitoring keystrokes, intersepting emails or other communication

31-01-24 →

* Denial of Service attack - (DOS)

- It aims to make a computer resource unavailable to its intended user.
- This typically accomplished by overwhelming the target resource with a large amount of traffic so that it becomes unavailable to legitimate user and they are conducted using single attacking system.

• mostly used protocol (ABS and DDDES)

• This result disription of server or degradation of performan or a complete shutdow n

• This attack can be launched from a single device or from a network of compromise devices. sometime called as botne

* Distributed denial of service attack - (DDOS)

• This type of cyber attack uses multiple compromise devices to flood the target resource with massive traffic making it unavailable to legitimate user.

• Unlike simple (DOS) attack or (DDOS) attack leverage the powe of multiple devices to generate a large volume of traffic.

• This type of attack generally launched from bottnet.

* TCP/IP Hijack :-

• In this attack the attack intersect or alter the transmi control protocol and intercept protocol packets that are been sent between to system b manipulating the sequence and acknoledgement no. in the TCP header.

• The attacker can take control of the communication, sessio and potentially redirect the flow of data

• To prevent TCP/IP hijack we use security protocol SSL (secure socket layer) or TSL (Transport security layer)

• B

* • BackDoor -

• It is a method of bypassing normal authentication processor to gain unauthorized access to a computer system.

*. Trapdoor :-

It is similar to backdoor in that it is a hidden method of bypassing normal authentical processor to gain unauthorized

access to computer system or network.

* Sniffing -

Sniffing can be perform on wired or wireless network and it is a significant security threat because it allows attacker to eaves drop on communication and gather sensitive information without the knowledge of user.

*. Replay Attack -

• Replay attack can occur in various scenario such as network communication where the attacker intersects and retransmit the message that is originally send by legitimate user.
• In this case the system received the replay message may process it as a new message and validate the unauthorized access.

*. Man in middle attack :-

• In this type of attack the attacker intersects and alters communication between two parties they are communicating directly with each other.
• In this attacker attacker secretly intersects and potentially alters an eaves drop communication between two party.

*. Information -

• Information refers to data or knowledge that is processed and store in a manner that is usable for decision making or problem solving.
• It can be in various forms such as text, numbers, image, audio or video.
• The rapid growth of the internet and other communication technologies has made it possible to access and share ~~worst~~ vast amount of information globally.

*. Information classification -

• There are several common type of information classification:-

1) Confidential
2) Sensitive
3) Public information
4) Top secret

*. Criteria ~~Top Secret~~ for information Classification:-

1) Several common factors that organization use to classify inform
or information classification includes:-
i) level of sensitivity
ii) legal requirements
iii) Business impact
iv) Possibility of harm
2) Organization can use these and other factors to determine appropriate level for information and to ensure that it is handled and protected appropriately.

*

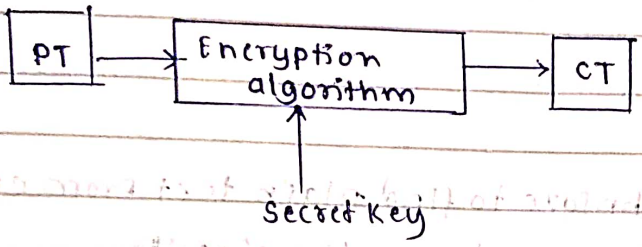
02-02-24

3 CRYPTOGRAPHY

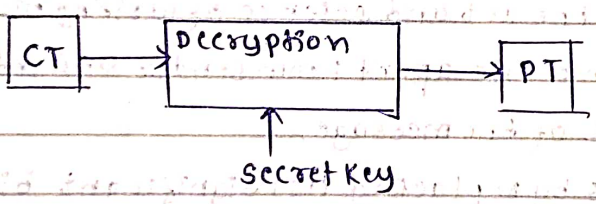
- Cryptography – It is the method of storing and transmitting data, so that it cannot be interpreted or understood.
- It is ~~sigma~~ science of protecting information by importing it into an unreadable format.

- Components of cryptography –

Encryption –



decryption



- PT → It is data in readable format or text to be Encrypted
- CT → Unreadable data created after Encryption. it is output of the encryption process.

- Encryption – it is a process of converting plain text to cipher text using secret key and encryption algorithm.

- Decryption – it is a process of converting cipher text to plain text using secret key and decryption algorithm.

- Encryption and Decryption Algorithm:-

i) It is a mathematical rule use in encryption or decryption.

ii) Properties of algorithm -

a) reversible

b) simple for calculation

c) Require less time for computation.

d) Difficult to crack o (secure)

- Crypt Analysis -

i) Crypt Analysis is a technique to find plain text from cipher te without the knowledge of key and encryption algorithm.

- STEGANOGRAPHY -

i) steganography is the art and science of writing hidden message in such a way that no one apart from sender and intended receiv suspect the existence of the message.

ii) steganography works by replacing last significant bits with bit of information to be hidden.

iii) This information can be on plain text, cipher text or even a image

iv) Media files are ideal for steganography because of their large size.

v) Steganography embeds a secret message in a covered message which is parameterized by stegokey

∴ cover media + hidden data + stego key - stego media.

vi) In order to get hidden message stego key is required.

- Application of STEGANOGRAPHY -

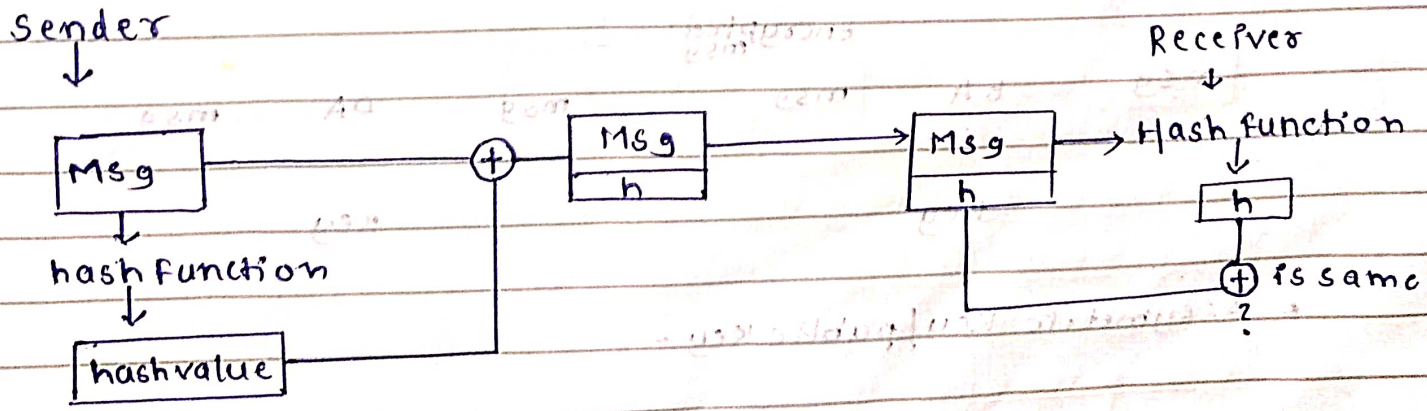
i) steganography is used by some model printers.
ii) steganography is used in digital watermarking.

- HASHING -

i) Hash function are mathematical algorithm that generates a message summary or digest to confirm the identity of a specific message that their have not been any change to the content hash function is not used to encrypt message but it is use to identify sender and check the integrity of the message.
ii) Hashing is characterized by the hash algorithm.
iii) A hash algorithm is publically known function that creates hash value also known as message digest by converting variable length message into single fixed length value.

Formula - H(M) = h

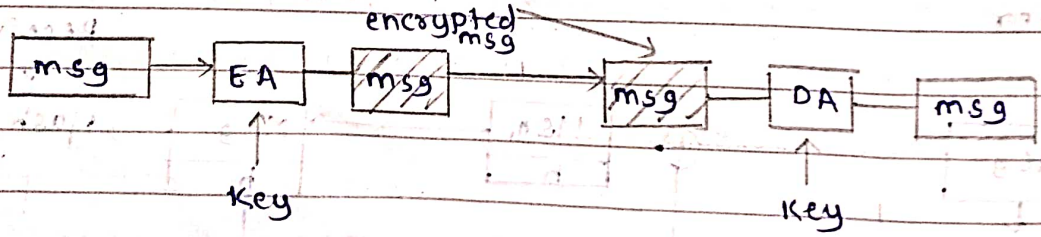
Where, M = message
H(M) is a hash function (Algo)
h → hash value.



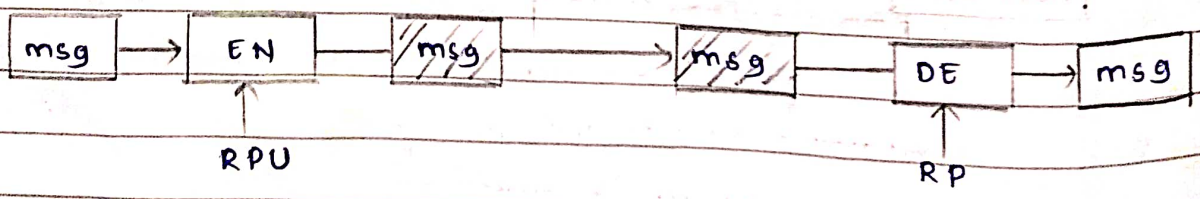
* Comparison between symmetric and Assymetric Key -

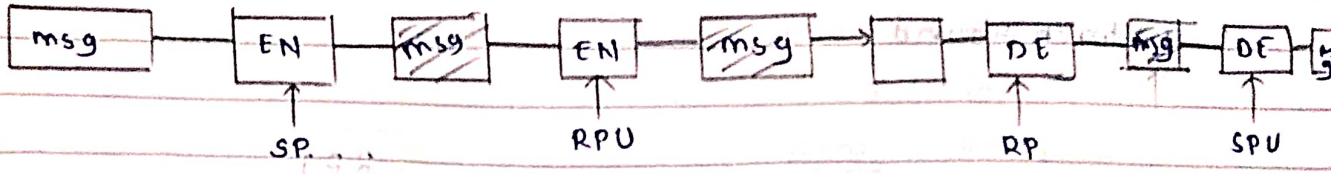
Category	Symmetric Key/Secret Key	Assymetric Key/Public Key
1) Key used for encryption & Decryption	i) Same key is used for encryption and Decryption.	i) One key is used for encryption and another key is used for Decryption
2) Key process	ii) Ke = Kd	ii) Ke ≠ Kd
3) Speed of Encryption	iii) It is fast	iii) It is slow as compare to symmetric Key
4) Key exchange ~~extend~~	iv) Key exchange is a big problem.	iv) Key exchange is easy.
5) No. of key required as compare to no. of participant	v) Equal to square of participants.	v) same as the no. of participant.
6) Uses	vi) Mainly for encryption and decryption.	vi) Digital signature and encryption, Decryption.
7) Example -	vii) DES (Data encryption standard), DDDES, Lowfish, ADS.	vii) RSA, Ealiptic curve crypto system, Diffiehellmen, Digital Signature stand (DSS).

* Symmetric key/secret Key -

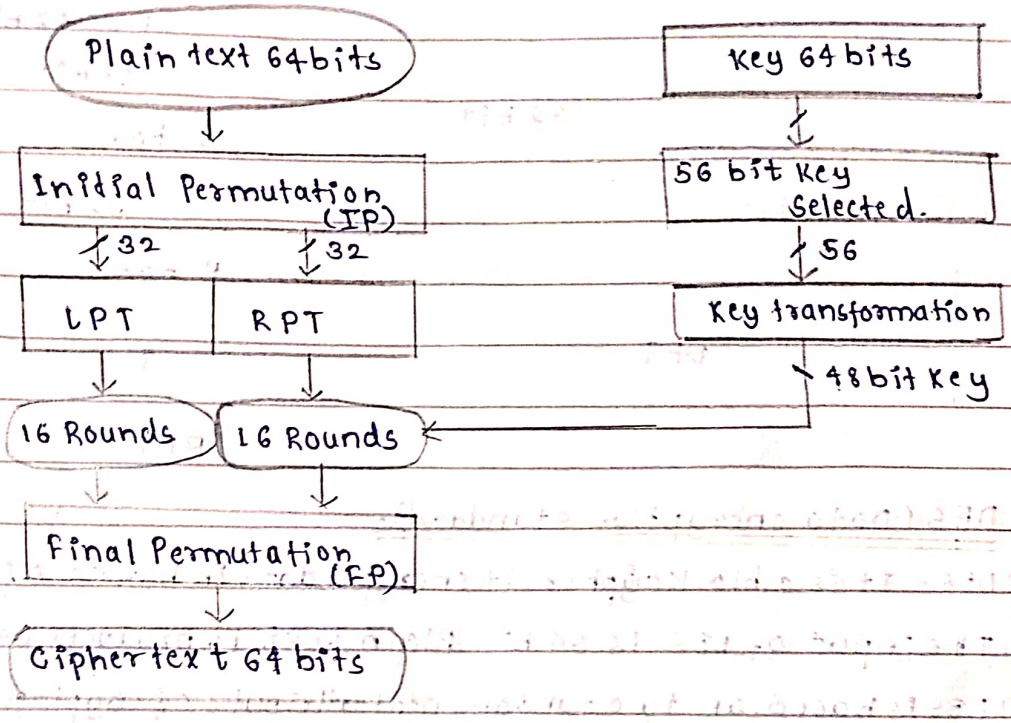


* Assymetric Key/public Key -

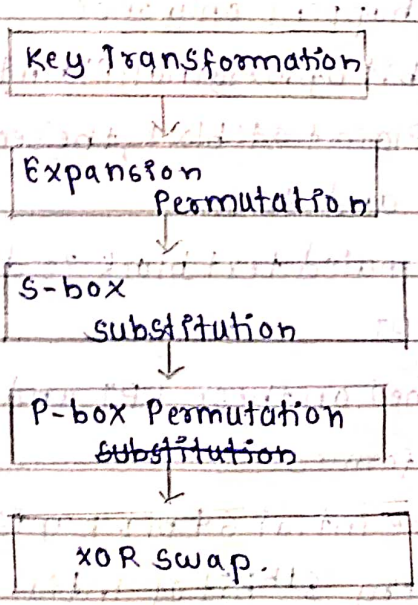




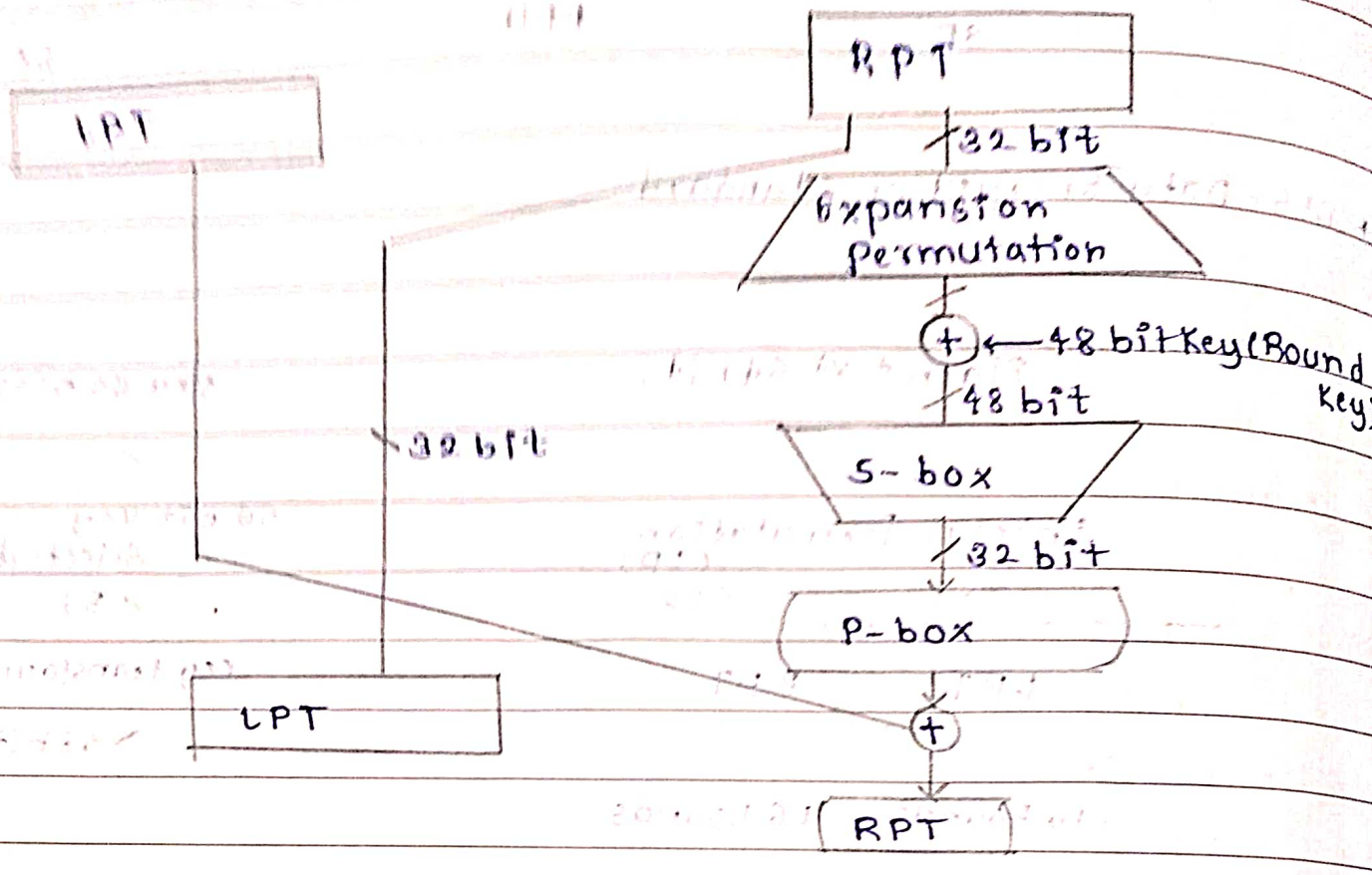
* DES - Data Encryption standard -



*. Each Round Steps -



* Each Round =



* DES (Data encryption standard) -

i) DES - It is a block cipher it encrypts data in blocks of size 64 bits.

ii) The input of DES is 64 bit Plain text it produces 64 bit ciphertext

iii) DES is based on two fundamental attributes of cryptography that is substitution and transposition.

iv) DES consist of following steps -

a) Initial Permutation - It happens only once.

- It replaces the first bit of original Plain text block with the 58 bit of the original Plain text block, the second bit 50th bit of the original pt block and so on.

b) The result in 64 bit permuted text block is divided into two halfs of 32 bit i.e LPT and RPT.

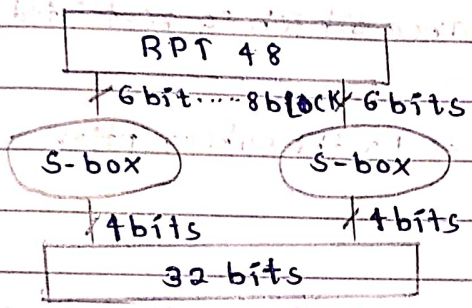
c) 16 rounds are performed on these LPT and RPT, in each round following steps are performed -

- Key transformation - The intial 64 bit key is transformed into 56 bit key by discarding every 8th bit of intial key.

Thus, for each round a 56 bit key is available

From this 56 bit key a different 48 bit sub key is generated during each round. this process is called as Key transformation.

- Expansion Permutation - During expansion Permutation the RPT is expanded from the 32-bit to 48 bits.
  The 32 bit RPT is divided into 8 blocks of 4 bit this 4 bit is expanded to 6 bit by adding two more bits.
- X-OR operation - The compressed 48 bit key and the expanded RPT (48 bit) are XOR.
- S-box - It accepts the input from X-OR operation and produces 32 bit output using substitution technique.



- P-box permutation - The output of S-box is provided to P-box, P-box permuted this 32 bits.
- X-OR and swap - The LPT of intial 64 bit is X-OR with the output produced by P-box the result of this X-OR operation becomes the new RPT and the old RPT becomes the new LPT.

d) Final Permutation - At the end of 16 rounds the final permutation is performed which is reverse of initial permutation.

2. Authentication AND Access CONTROL

- Password Attacks -
  i) piggybacking
  ii) Shoulder surfing
  iii) Dumpster diving

i) Piggybacking -

- piggybacking is the simply gaming access of a wireless connection closely behind a person who just used his own access card or pin to gain physical access to a room or building without the knowledge of the person.
- It is used to gain access do the area which is restricted.
- It is used to hide identity.
- Sometimes it is used to avoid fees to the subscription.

ii) Shoulder Surfing -

- Shoulder surfing refers to direct observation technique, where unauthorized user try to gain information by looking overs someone's shoulder.
- This method is effective in crowded places because it is relatively easy to observe.
- Someone's activities like entering pin or password filling out information form etc. Shoulder surfing can be done from a distance by using vision enhancement devices.
- To avoid shoulder surfing it is a device to hide keypad by using body.
- Donot used computers in crowded places like cyber cafe, library or places where people are closed to you.

iii) Dumpster diving -

- In dumpster diving all the attacker search for important system information by searching the dump.
- The search is carried out in paper waste, electronic waste, such as old hard disk, floopy disk, CD, DVD's etc....
- Attacker try to extract password, system configuration, network configuration, users information etc...
- By using this information the attacker may gain access to system.
- expert recommend that company should have policies to dispox of waste properly.

* . Unauthorized software or hardware Installation.

*. . individual user responsibilities

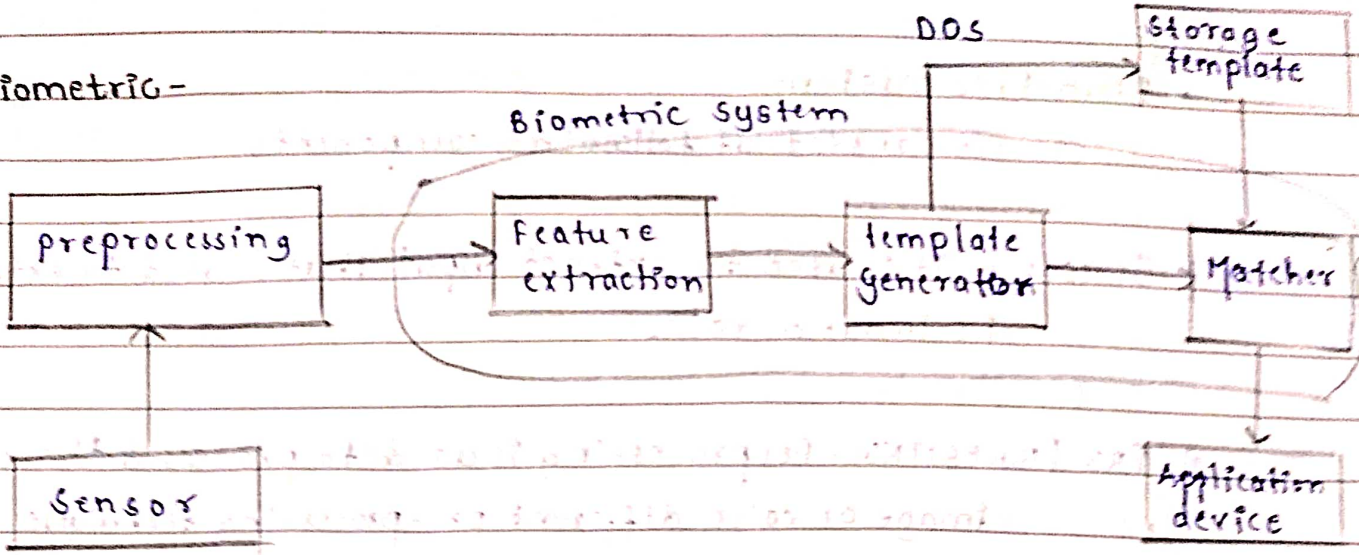
* . access control.

- Identification, Authentication -

Methods of choosing password -

21-02-24

* Biometric -



- Biometric - it refers to study of methods of uniqely recognizing human based upon one or more physical or behavioral characters.

Biometric

physical
- face
- fingerprint
- Iris
- DNA
- Handprint

Behavioral
- keystroke
- voice
- signature.

- Human characteristics are used for biometric recognition because of following characteristics -

1) universal -
2) Uniqueness -
3) easily collectable -
4) Performance -
5) acceptability -

Imp-

- Biometric system -
  it consist of following components -

1] SENSOR = It is used to extract input that is used to extract i.e image or voice.

2] PRE-PROCESSING - Preprocessing is used to processed the extract image or voice. different pre-processing techniques are used like
   i) normalization
   ii) Dilation
   iii) conversion into specific type - greyscale or black and

3] FEATURE EXTRACTION - Is used to extract required feature from the preprocessed image.

4] TEMPLATE GENERATOR - The template generator generates template using the features extracted and store it into the database while enrolling

5] MATCHER - matcher matches the template generator and template stored in the database if the matching is stablished between the template generated and in the template in database and then access to the application is granted.

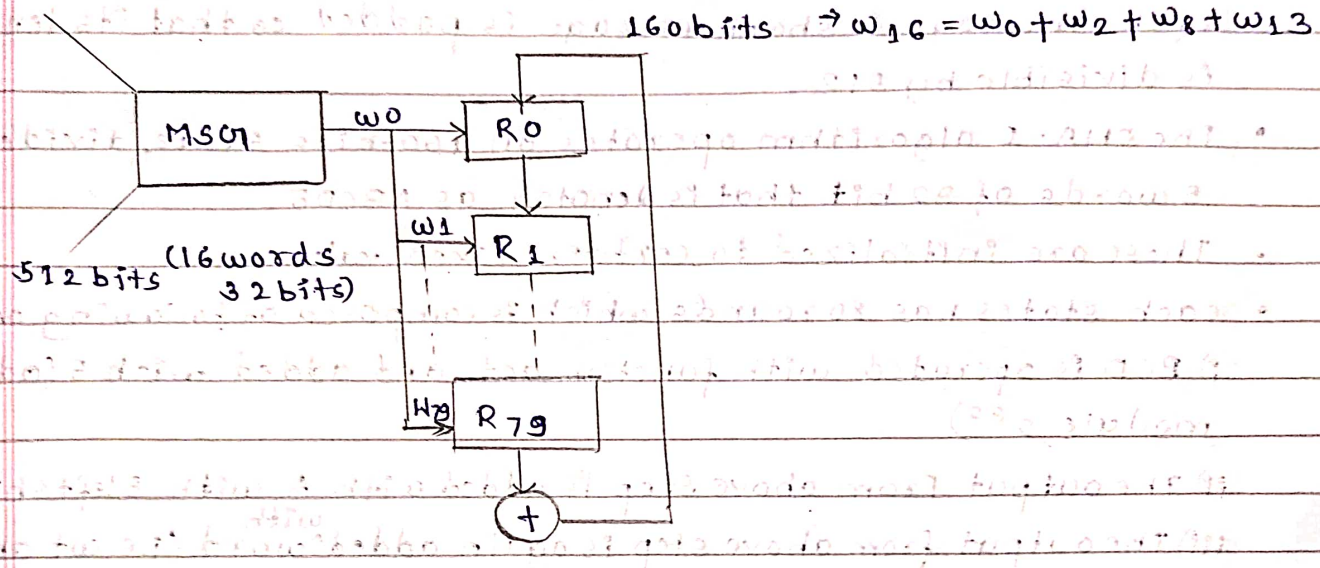
- Biometric works on following two modes -

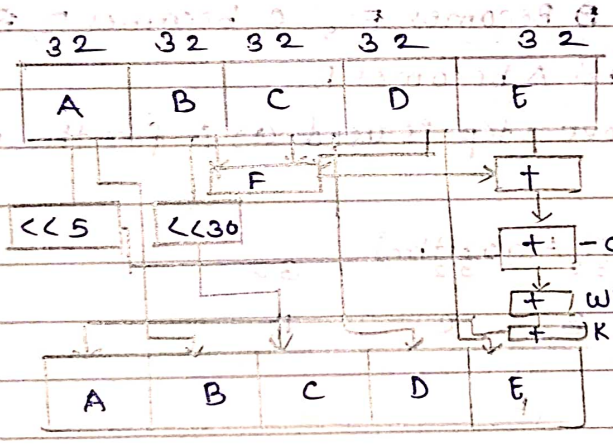
1) Verification -
2) Identification -

- Verification - A one to one comparison of a capture biometric with a stored template to verify the individual.

- Identification - A one to many comparison of the captured biometric against a bio-metric database.

* SHA-1 - (Formula - $wt = wt-16 \oplus wt-14 \oplus wt-8 \oplus wt-3$)





A = H0 = 67452301

B = H1 = EFCDAB89

C = H2 = 98BACDFE

D = H3 = 10325476

E = H4 = C3D2E1F0

K_1t = 5A827999 0 to 19 - B.C ∧ $\bar{B}$.D

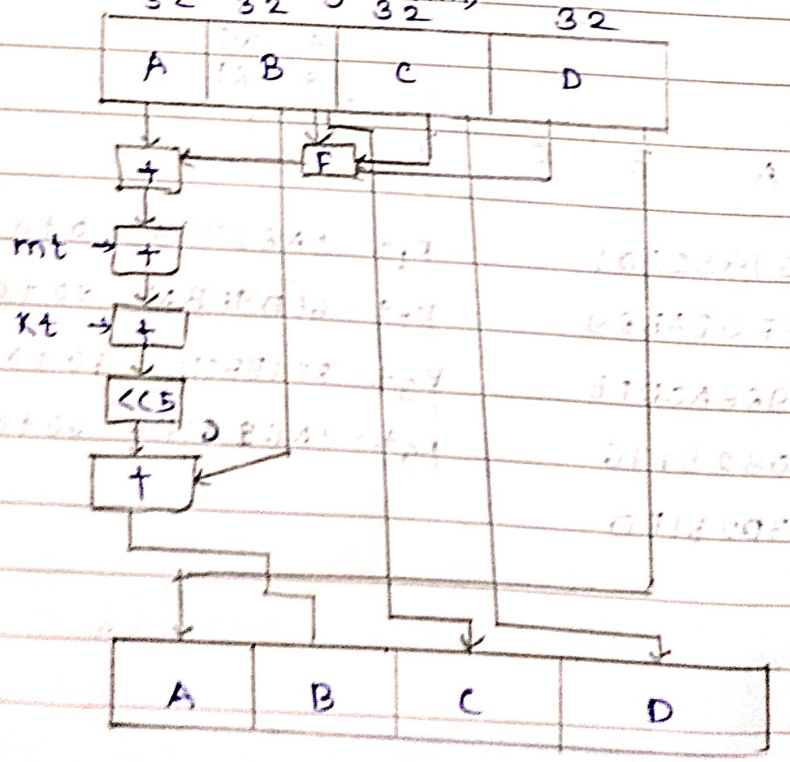
K_2t = 6ED9EBA1 20 to 39 - B⊕C⊕D.

K_3t = 8F1BBCD 40 to 59 → B.C ∧ B.D ∧ C.D.

K_4t = CA62C1D6 60 to 79 → B⊕C⊕D

- one of the algorithm is use in public key encryption is secure hash algorithm (SHA-1 → 160 bit), (SHA-2 → SHA-256 and SHA-
- In SHA-1 the message is of variable length which is divided into chanks of 512-bits (i.e 16 words of 32 bits).
- If the message is short message is padded so that its length is divisible by 512.
- The SHA-1 algorithm operates on 160-bits state, divided in 5 words of 32 bit that is denoted as ABCDE.
- These are initialized to certain fixed value.
- each states has 80 rounds which is composed of following opera
  i) BCD is operated with function act and added with E (additio module 2^{32})
  ii) The output from above step is added with A with 5 leftshift.
  iii) The output from above step is again added with word (i.e wt and K i.e KT)
  iv) For the next round B becomes E, C becomes D, B becomes C with 30 left shift and A becomes B.
  ∴ (The output from above step is used as A for the next round)

* MD-5 - (message digest Algorithm)



- Is a widely used cryptographic hash function with a 128 bit hash value.
- The variable length input message is broken down into chunks of 512 bits (i.e 16 words of 32 bits).
- The message is padded so that its length is divisible by 512.
- The ~~process of message blocks~~ Algorithm operates on 128 bits state divided into 4 words of 32 bits. denoted by ABCD. These are initialised a certain fixed constants.
- The algorithm than use each 512 bit message block in terms to modify the state.
- The processing of message block consist of 4 similar stages, terms round and each round is composed of 16 similar operation based on non-linear F, modular addition and left rotation.